IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB8995

Chapter VIII

New Challenges in Privacy Protection

Lech J. Janczewski
University of Auckland, New Zealand

ABSTRACT

The protection of privacy is a function of many variables: culture, politics, and point of view. Practically all countries have introduced laws regulating these problems. Terrorist attacks culminating with the destruction of the World Trade Center in New York and the Pentagon in Washington indicated a need to change these regulations. Therefore, this chapter defines the notion of privacy and cites typical regulations related to the protection of privacy and the interception of private communications and documents. This discussion terminates with a presentation of a worldwide prognosis in this field.

INTRODUCTION

The attack against major US businesses and military facilities on September 11, 2001 had and still has a major effect on the way the entire civilized world functions. During the writing of this text, it is impossible to predict the final outcome of military actions launched against the people responsible for the attack or those who sheltered them. However, without a doubt, we witness a major shift in the attitude towards protection of the interests of individuals.

In the past, the focus of the law was aimed at protecting the privacy of individuals by setting up standards related to spreading the information concerning individuals and/or the interception of mail. Growing utilization of the Internet, and more generally, computer systems and networks made most of these regulations non-functional, as significant parts of the data are transported or stored in the electronic form.

In the case of traditional documents, the process of privacy protection continues to be well regulated. A majority of countries have introduced laws detailing rules on how to preserve the privacy of individuals while still allowing law enforcement agencies to carry out their duties. Of course, the range of the activities carried out by these agencies varies from country to country, however, in the case of democratic countries, the differences are rather secondary.

This balanced process was disturbed in the last decade by two factors:

- the mass implementation of computers and Internet technology; and
- the development of worldwide terrorist networks and other outlawed organizations.

In the past, privacy protection of the communication processes was based on trust in the postal organizations not allowing unauthorized individuals or organizations to intercept and read the messages. On the other hand, the technologies of reading the sealed letters were trivial. All of us know that steam coming from a kettle is an excellent way to open letters! Progress in electronic communications dramatically changed this. More independent organizations are involved in the process of message transportation. From this point of view, interception of messages is much easier. But there is the other side of the coin—it is easier to limit unauthorized access to information through use of encryption or the use of steganography techniques. Steganography technique is a procedure for hiding given information within the other data. Wolf (2001) gave an example of such a process, where hiding almost 2K of data in a picture file would not change the appearance of the picture at all.

The best illustration of this process is the information related to the operation of Osama bin Laden's al-Qaeda network. French police in Paris intercepted a scribbled notebook belonging to a suspected master bomber. FBI and French computer experts studied the Arabic script and are convinced that terrorist cells have been using codes to disguise their electronic mail and to hide maps and instruction in sports chat rooms, pornographic websites, and photographs sent over the Internet. Hence, intelligence agencies are certain that al-Qaeda uses electronic camouflage to keep in touch with its network of agents (Zalewski, 2001).

On the one hand we have witnessed the growing utilization of computer networks for conducting fraud operations, and on the other hand, we have the growing concern of society, as it becomes aware its privacy could be the first casualty of the "War on Terror." All indicators show that computer fraud and illegal access to information are on the rise. This trend is clearly seen in the "CSI/FBI Annual Security Report" prepared jointly by the Computer Security Institute and the Federal Bureau of Investigation (CSI/FBI, 2002). According to this report, for the last five years the financial losses resulting from computer/network abuse are on the increase.

In this chapter, it is not our intention to present an opinion about the required level of individuals' privacy protection, for instance, whether it is moral or not to read somebody's private correspondence. Rather, the objective of this chapter is to present:

- the mechanisms that currently exist around the world in this field, with focus on the law related to privacy protection;
- the public perception of these mechanisms;
- the demonstrated tendencies; and
- what they could mean for the world community.